



Building Incident Handling Capabilities: Organizational Models

CERT® Coordination Center
Networked Systems Survivability
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

© 2001-2004 Carnegie Mellon University
® CERT, CERT Coordination Center, and Carnegie Mellon are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University

This material is approved for public release. Distribution is limited by the Software Engineering Institute to attendees.

The CERT® Coordination Center (CERT/CC) was created in November 1988 by the Defense Advanced Research Projects Agency (DARPA) in the aftermath of an Internet Worm incident.

The CERT/CC is located at Carnegie Mellon University's Software Engineering Institute (SEI). The SEI is a federally funded research and development center (FFRDC) sponsored by the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics [OUSD (AT&L)].

The mission of the CERT/CC is to

- act as a coordination center,
- foster collaboration across the network community to achieve effective incident response,
- assist other organizations in forming response teams, and
- conduct research and analysis of incident trends.



Who We Are: The CERT CSIRT Development Team (CDT)

CERT® Training and Education
Promote the widespread adoption of security practices and increase the quality and quantity of practitioners, managers, and educators.

Our mission:

- Foster a user community that is aware, knowledgeable, trained, and educated about information assurance and survivability.
- Improve the ability of technical staff, managers, and senior executives to ensure survivability of critical information assets and systems.
- Identify best known current practices for protecting networked systems and managing incidents when they occur.
- Develop and transition products based on the CERT operational expertise and experiences with our customer community.

© 2001-2004 Carnegie Mellon University

© 2001-2004 Carnegie Mellon University

NASCIO Presentation - March 26, 2004 - slide 2

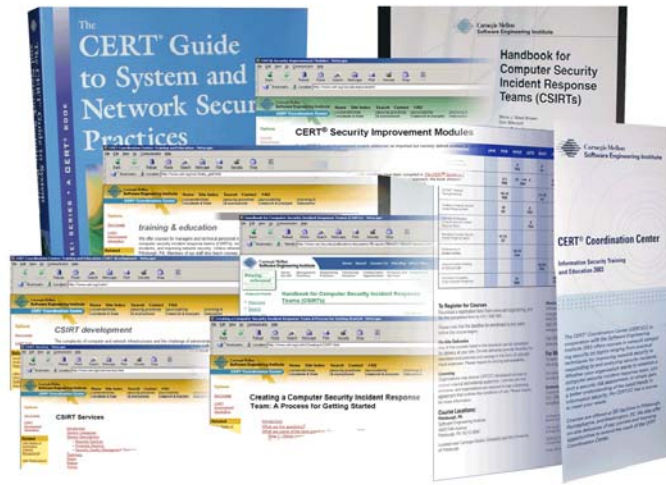
The CERT CSIRT Development Team is part of the CERT Education and Training area of the Networked Systems Survivability Program within the Software Engineering Institute.

Our CSIRT Development Team Vision and Mission

- Vision
 - Sufficient CSIRTs exist to meet the demand to protect the resources of the organizations they support.
- Mission
 - Foster the growth of global incident response capabilities.
 - Assist national and international organizations in establishing effective CSIRTs.
 - Help existing CSIRTs improve their services and operation through training, mentoring, and collaboration.



What Do We Do?



<http://www.cert.org/csirts/>

© 2001-2004 Carnegie Mellon University

NASCIO Presentation - March 26, 2004 - slide 3

The CERT CSIRT Development Team helps organizations build their own computer security incident response teams (CSIRTs) and also helps existing teams enhance their effectiveness. The team is an outgrowth of the work and products developed in the CERT Coordination Center (CERT/CC). Our focus is to assist new and existing teams in understanding best practices and recommendations for performing incident handling and related CSIRT services. The guidance provided is based on the history and experiences of the CERT/CC, along with knowledge gained from our extensive collaborations with other teams.

To help organizations, we

- research the current incident management environment, looking to synthesize existing information and best practices into guides, standards, and methodologies for performing incident handling processes and functions
- work with teams to
 - develop strategies to plan and implement CSIRTs
 - develop best practices for operating CSIRTs
 - adopt CSIRT policies and standard operating procedures
- collaborate with teams to develop publications, guides, templates, and checklists to assist in the incident handling process
- develop and teach courses related to CSIRTs
- license courses to organizations and train their trainers to deliver the materials
- provide a CERT-Certified Computer Security Incident Handler certification

For more information, please contact csirt-info@cert.org.



What is a CSIRT?

An organizational capability or team that provides services and support, to a defined constituency, for preventing, handling and responding to computer security incidents



© 2001-2004 Carnegie Mellon University

NASCIO Presentation - March 26, 2004 - slide 4

Even the best information security infrastructure cannot guarantee that intrusions or other malicious acts will not happen.

- When computer security incidents occur, it will be critical for an organization to have an effective means of responding.
- The speed with which an organization can recognize, analyze, and respond to an incident will limit the damage done and lower the cost of recovery.

Much like a fire department, a CSIRT can perform both reactive and proactive services.

A fire department responds to and extinguishes fires. They also proactively provide fire-prevention training, promote the installation of smoke alarms and purchasing of fire escape ladders, and instruct families in the best manner to safely exit a burning building.

The benefits of a CSIRT include

Reactive

- focused response effort
- more rapid, standardized, and coordinated response
- stable cadre of staff with incident handling expertise, combined with functional business knowledge
- collaboration with others in security community

Proactive

- enables organizational business goals
- provides authentic risk data and business intelligence
- provides input into product development cycle or network operations
- assists in performing vulnerability assessments, developing security policies, and providing awareness training



What Does a CSIRT Do?

In general a CSIRT

- **provides a single point of contact for reporting problems**
- **identifies and analyzes what has happened including the impact and threat**
- **researches solutions and mitigation strategies**
- **shares response options, information, and lessons learned**

A CSIRT's goal is to

- **minimize and control the damage**
- **provide or assist with effective response and recovery**
- **help prevent future events from happening**

No single team can be everything to everyone!

© 2001-2004 Carnegie Mellon University

NASCIO Presentation - March 26, 2004 - slide 5

The goal of a CSIRT is to minimize and control the damage, provide effective response and recovery, and work to prevent future events from happening.

The goals of a CSIRT must be based on the business goals of the constituent or parent organizations. Protecting critical assets are key to the success of both an organization and its CSIRT.

CSIRTs can be on site and able to conduct a rapid response to contain and recover from a computer security incident. CSIRTs may also have familiarity with the compromised systems and therefore be more readily able to coordinate the recovery and propose mitigation and response strategies. Their relationships with other CSIRTs and security organizations can facilitate sharing of response strategies and early alerts to potential problems.

CSIRTs started as “response-oriented” organizations, but have since developed into organizations that work proactively to defend and protect the critical assets of organizations and the Internet community in general. This proactive work includes providing security awareness and education services, influencing policy, and coordinating workshops and information exchanges. It also includes analyzing intruder trends and patterns to create a better understand of the changing environment so that corresponding prevention, mitigation, and response strategies can be developed and disseminated.

CSIRTs can work with other areas of the organization to ensure new systems are developed and deployed with “security in mind” and in conformance with any site security policies. They can help identify vulnerable areas of the organization and in some cases perform vulnerability assessments and incident detection.



Variety of CSIRTs Across the Globe



The number of CSIRTs continues to increase across the globe. These CSIRTs come in a variety of organizational structures and provide a diverse set of services.

General categories of CSIRTs include

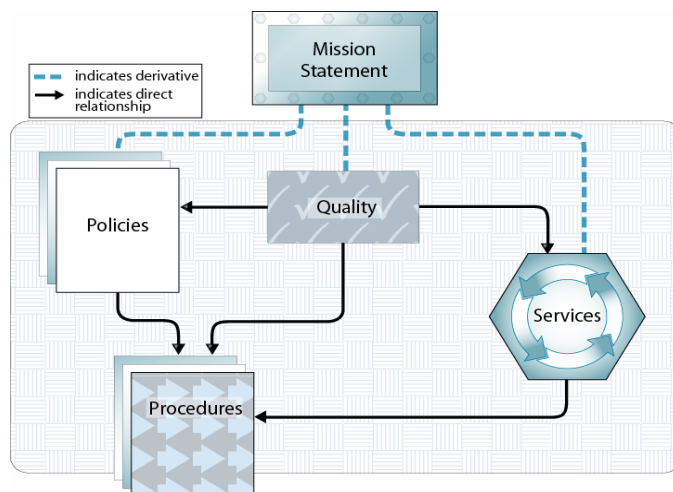
- Internal CSIRTs - provide incident handling services to their parent organization; this could be a CSIRT for a bank, a university, or a federal agency.
- Coordination Centers – coordinate and facilitate the handling of incidents across various CSIRTs, or for a particular country, state, region, province, research network, or other such entity. Usually will have a broader scope and a more diverse constituency.
- Analysis Centers – focus on synthesizing data from various sources to determine trends and patterns in incident activity. This information can then be used to help predict future activity or provide early warning when current activity matches a set of previously determined characteristics.
- Vendor Teams – coordinate with organizations who report and track vulnerabilities; another type of vendor team may provide internal incident handling services for their own organization.
- Incident Response Providers – provide incident handling services as a product to other organizations. These are sometimes referred to as Managed Security Service Providers (MSSPs).

Various global and regional organizations devoted to incident management collaboration and coordination have been created. This includes organizations such as the

- Forum of Incident Response and Security Teams
<http://www.first.org/>
- TF-CSIRT - Collaboration of Security Incident Response Teams (Europe)
<http://www.terena.nl/tech/task-forces/tf-csirt/>
- Asian Pacific Computer Emergency Response Team (APCERT)
<http://www.apcert.org>



Creating an Effective CSIRT



© 2001-2004 Carnegie Mellon University

NASCIO Presentation - March 26, 2004 - slide 7




To be effective, a CSIRT requires four basic elements.

- operational framework
 - clear mission
 - defined constituency
 - organizational home
 - formal relationship to other organizational teams
- service and policy framework
 - defined services
 - defined information flow
 - defined process for collecting, recording, tracking, and archiving information
 - clear, comprehensive organization-wide policies
- effective quality assurance practices
 - definition of a quality system
 - specific measurements and checks of quality parameters
 - reporting and auditing practices and procedures
 - balance, compliance, and escalation procedures to ensure quality levels
 - constituency and customer feedback
- adaptability and flexibility
 - ability to adapt to real-time threats and future emerging threats
 - legal expertise and support

These elements help to define the basic requirements and benchmarks against which a CSIRT can evaluate its operation and effectiveness.



Range of CSIRT Services

Reactive Services 	Proactive Services 	Security Quality Management Services 
<ul style="list-style-type: none"> + Alerts and Warnings + Incident Handling <ul style="list-style-type: none"> - Incident analysis - Incident response on site - Incident response support - Incident response coordination + Vulnerability Handling <ul style="list-style-type: none"> - Vulnerability analysis - Vulnerability response - Vulnerability response coordination + Artifact Handling <ul style="list-style-type: none"> - Artifact analysis - Artifact response - Artifact response coordination 	<ul style="list-style-type: none"> ○ Announcements ○ Technology Watch ○ Security Audit or Assessments ○ Configuration & Maintenance of Security Tools, Applications, & Infrastructures ○ Development of Security Tools ○ Intrusion Detection Services ○ Security-Related Information Dissemination 	<ul style="list-style-type: none"> ✓ Risk Analysis ✓ Business Continuity & Disaster Recovery Planning ✓ Security Consulting ✓ Awareness Building ✓ Education/Training ✓ Product Evaluation or Certification

© 2001-2004 Carnegie Mellon University

NASCIO Presentation - March 26, 2004 - slide 8

Here is an example of the types of services a CSIRT might choose to offer. Not all CSIRTs provide the same set of services. This slide lists some common services that a team could provide. They can also be found in the online version of this document at

<http://www.cert.org/csirts/services.html>

For a team to be considered a CSIRT, it must provide an incident handling service. That means it must provide at least one of the incident handling activities: incident analysis, incident response on site, incident response support, or incident response coordination.

According to this list, CSIRT services can be grouped into three categories:

Reactive service.

- These services are triggered by an event or request, such as a report of a compromised host, wide-spreading malicious code, or something that was identified by an intrusion detection or network logging system. Reactive services are the core component of incident handling work.

Proactive services.

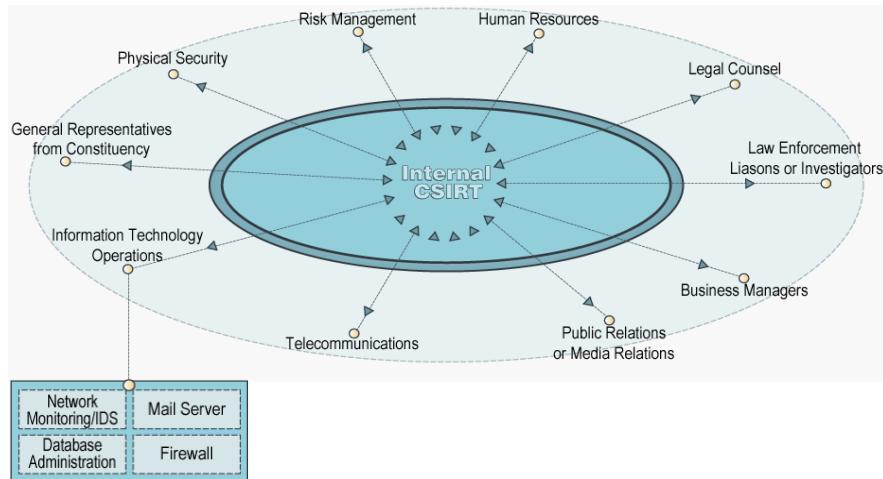
- These services provide assistance and information to help prepare, protect, and secure constituent systems in anticipation of future attacks, problems, or events. Performance of these services will directly reduce the number of incidents in the future. These services are ongoing, rather than being triggered by a direct event or request.

Security quality management services.

- These services augment existing and already well-established services that are independent of incident handling and traditionally have been performed by other areas of an organization such as the IT, audit, or training department. If the CSIRT performs or assists with these services, the CSIRT's point of view and expertise can provide insight to help improve the overall security of the organization and identify risks, threats, and system weaknesses. These services are generally proactive in nature but contribute indirectly, rather than directly, to a reduction in the number of incidents.



Who Needs To Be Involved: Internal CSIRT



© 2001-2004 Carnegie Mellon University

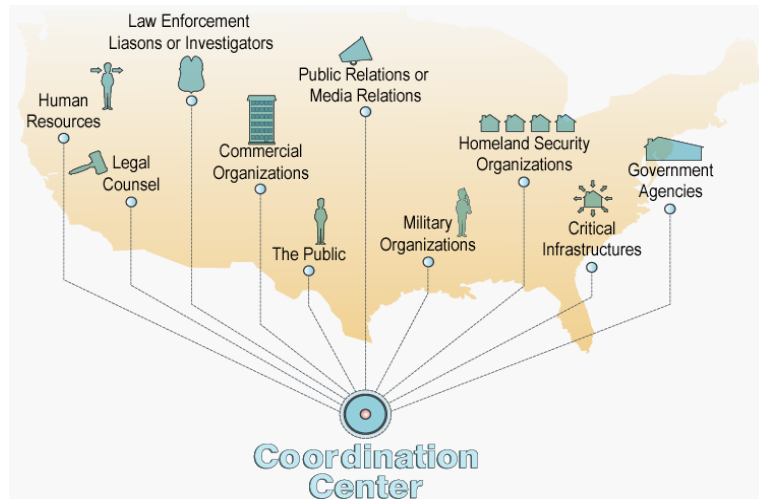
NASCIO Presentation - March 26, 2004 - slide 9

Incident Handling is not a self-contained process. Relationships, communication channels, data sharing agreements, and policies and procedures must be established across the organization. For an internal team, this includes

- Business managers. They need to understand what the CSIRT is and how it can help support their business processes. Agreements must be made concerning the CSIRT's authority over business systems and who will make decisions if critical business systems must be disconnected from the network or shut down.
- Representatives from IT. How will the IT staff and the CSIRT interact? What actions will be taken by IT staff and what actions are taken by CSIRT members? What information can the IT staff provide to the CSIRT and what information the CSIRT can provide to the IT team? What roles and authority do each have?
- Representatives from the legal department. When and how is the legal department involved in incident response efforts?
- Representatives from human resources. They will need to be involved in developing policies and procedures for removing internal employees found engaging in unauthorized or illegal computer activity.
- Representatives from public relations. They must be prepared to handle any media inquiries and help develop information disclosure policies and practices.
- Any existing security groups, including physical security. The CSIRT will need to exchange information with these groups about computer incidents and may share responsibility with them for resolving issues involving computer or data theft.
- Audit and risk management specialists. They can help develop threat metrics and risks to constituency systems.
- Any law enforcement liaisons or investigators. They will understand how the team should work with law enforcement, when to contact them, and who will do the investigations or even forensic analysis.
- General representatives from the constituency. They can provide insight into their needs and requirements.



Who Needs To Be Involved: Coordination Center



© 2001-2004 Carnegie Mellon University

NASCIO Presentation - March 26, 2004 - slide 10

For teams that serve as a coordination center or support a state, national, provincial or similar government entity constituency – it is even more difficult to determine how the relationships with the participating organizations should be structured.

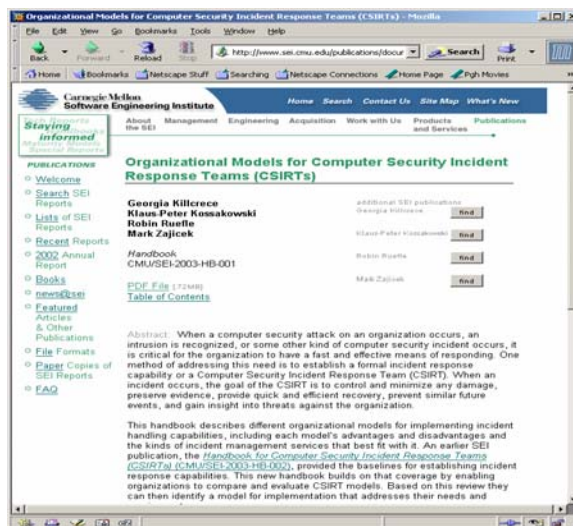
Will the CSIRT only deal with particular organizations such as

- government organizations
- military organizations
- critical infrastructures
- business organizations

Or will the CSIRT accept reports from and disseminate information to the public?



Organizational Models for CSIRTs Handbook



© 2001-2004 Carnegie Mellon University

NASCIO Presentation - March 26, 2004 - slide 11

When designing the vision for a CSIRT, a model must be developed that defines how the CSIRT will operate and interact with the organization and constituency.

This model should take into account

- interactions that must take place
- information flows
- internal staff and external parties to be involved
- location of CSIRT staff
- requirements and needs of the constituent or organizational sites
- infrastructure for these interactions

Questions to be answered include

- What information will the CSIRT provide to the constituency?
- What information will the constituency provide to the CSIRT?
- How will the CSIRT interact with any information technology department?
- How will the CSIRT fit into any change management process?
- How will the CSIRT work with the investigative or law enforcement group?
- How will the CSIRT make recommendations for changes to internal and external defenses like firewalls or IDS?
- Who will host the CSIRT or where will the CSIRT report organizationally?

A CSIRT could be located in the IT or telecommunications department, the security group, the audit and compliance group or be its own unit. A CSIRT could report to the CEO, the CIO, the CSO, or another equivalent manager.

It is important to think about what actions the CSIRT will need to take and what type of management support will be required to facilitate those actions during incident handling and response. Identifying such issues may suggest the right reporting or management structure.



CSIRT Organizational Models

- **Security Team** - incident handling is done ad hoc by those in the organization responsible for system and network infrastructures.
- **Internal Distributed Team** – utilizes existing staff to provide a “virtual” distributed CSIRT, formally chartered to deal with incident response activities.
- **Internal Centralized Team** – a centrally located, dedicated CSIRT that provides incident handling services.
- **Internal Combined Distributed and Centralized Team** – a combination of the distributed CSIRT and the centralized CSIRT.
- **Coordinating CSIRT** – coordinates and facilitates the handling of incidents across a variety of internal or external organizations.

© 2001-2004 Carnegie Mellon University

NASCIO Presentation - March 26, 2004 - slide 12

Each type of CSIRT Model has its strengths, weaknesses, and benefits.

There are a variety of different models.

The model that is chosen will be based on

- where the constituency is located
- where the team is located
- what services are provided
- what information needs to be shared
- what type of actions need to take place

More than one organizational model may be needed. For example, a large, geographically dispersed organization might require local teams on site, reporting to a regional, centralized CSIRT with each regional CSIRT then reporting to a Coordination Center who then passes synthesized information to an Analysis Team for further research on trends and patterns

Models also may evolve over time. One important thing to remember is that a CSIRT may not be able to do everything at once. Resources and new services may need to be added in an incremental fashion. Many teams start out only providing Incident Handling services and grow into other services and other models as resources, budgets, and support allow. The organizational model may need to be revised over time based on changes in the CSIRT's mission, priorities, provided services, or sponsorship.



Internal Distributed CSIRT

Description

- local teams with CSIRT manager

Strengths

- defined plan, roles, and responsibilities
- information sharing can occur to create comprehensive analysis across the organization
- on-site reaction time can be faster time

Weaknesses

- time commitments can be an issue
- difficult to create a team synergy
- difficult to enforce consistent response effort

© 2001-2004 Carnegie Mellon University

NASCIO Presentation - March 26, 2004 - slide 13

An internal distributed CSIRT model is composed of staff from other divisions or sectors of the enterprise who report to a central CSIRT manager. The CSIRT is a formally recognized entity and has been given the responsibility for handling all incident response activities. The team is considered "internal" because it is a team within a particular organization or company, so it is internal to the enterprise.

The CSIRT manager reports to high-level management, such as a CIO, CSO, CRO, or the equivalent. While the CSIRT manager has a "centralized" office (in organizational terms), the team members are scattered across the organization's geographic and divisional locations. Members of the team are chosen based on their experience and expertise with various operating system platforms, technologies, applications, and security practices. Team members include systems and business experts, network engineers, and others who have the needed functional knowledge.

The distributed CSIRT serves two purposes: (1) it provides a broad base of expertise across all the systems in the enterprise and (2) it gives the CSIRT a foothold in each division to not only coordinate activity but promote following best practice security policies and response steps. In this way, members of the team are out in the field (i.e., local sites); they are the eyes and ears of the CSIRT. They are also the arms and legs of the CSIRT, as they will be the ones to perform the response or provide guidance to those who will be performing the response. The distributed CSIRT staff have first-hand, real work experience concerning the operations and issues facing the organization. This brings a practical view of what techniques and approaches will work to mitigate problems.

Supported Constituency

- This type of model is found in large, distributed organizations such as multinational corporations, government organizations, and educational institutions.
- This model especially can be found in commercial organizations with multiple sites and locations.
- In most cases, small organizations would not be best served by this model.



Internal Combined Centralized and Distributed CSIRT

Description

- a centralized team with distributed members across geographic or functional sites

Strengths

- best of centralized and distributed models
- mechanism for information sharing, analysis, and standardized responses

Weaknesses

- two structures to maintain
- still difficult to ensure conformance

© 2001-2004 Carnegie Mellon University

NASCIO Presentation - March 26, 2004 - slide 14

In this model a dedicated, centralized CSIRT is established that interacts with team members who are distributed throughout the organization in various geographic sites and divisions. The centralized team provides high-level analysis and recommends recovery and mitigation strategies. It also provides incident, vulnerability, and artifact response support for the distributed team members and other parts of the enterprise. The distributed team members at each site implement the strategies and provide expertise in their areas of responsibility.

This model maximizes the utilization of existing staff in strategic locations throughout the organization with the centrally located coordinating capability of the dedicated team to provide a broader understanding of the security threats and activity affecting the constituency. It has management support in assigning needed resources during times of crisis.

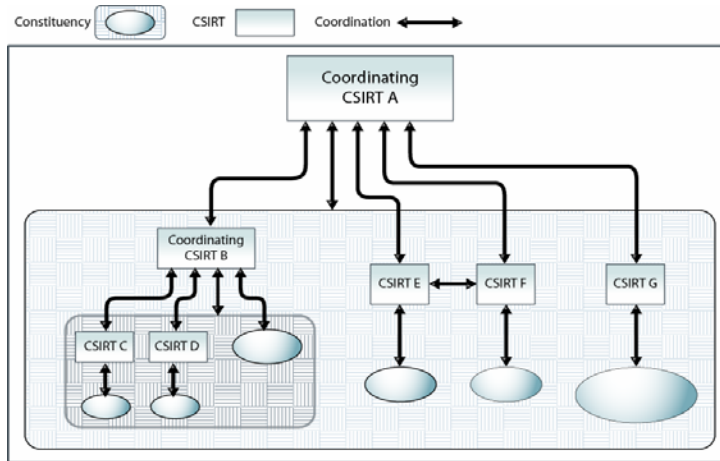
It builds on the infrastructure and expertise in the local areas where the distributed team members facilitate incident analysis and response (working with others in the organization—system, network, and security administrators, software developers, LAN/WAN managers, etc.—who are not part of the CSIRT). The CSIRT responds to reports of abnormal activity or other incident reports, participates in incident and vulnerability analyses, lends expertise in testing or assessing the security of the enterprise, and plays a proactive role in promulgating computer security awareness and training throughout the organization.

Supported Constituency

- This model works best for very large distributed organizations or constituencies; this might include a federal or state agency CSIRT, a multi-campus educational institution, or a multi-site commercial organization.
- Although conceptually this model will work in a small organization, it is probably not necessary, and a centralized model would work better.



Coordinating CSIRT



© 2001-2004 Carnegie Mellon University

NASCIO Presentation - March 26, 2004 - slide 15

A CSIRT can also be organized as a coordinating center rather than a one-on-one incident response service. In this case, the CSIRT helps facilitate incident handling and analysis efforts across dispersed, geographic teams or even across business units and departments throughout an organization. These dispersed groups carry out the actual incident response steps and mitigation strategies. The coordinating CSIRT synthesizes incident reports and statistics from all areas to determine the general security position of the organization and its vulnerability to attack. It also is able to consolidate the information so that an accurate picture of incident activity across the organization can be relayed as needed.

Coordinating CSIRTs facilitate information sharing and dissemination relating to

- incident trends, patterns, and activity
- response and mitigation strategies
- analysis and research
- new tools and techniques for incident handlers

Some questions to be asked

- Who will report incidents and information to the CSIRT?
- Who will receive notification, information, and support from the CSIRT?

Supported Constituency: organizations that share some common characteristics that make them part of the team's constituency. Common characteristics that are usually found today are

- network connectivity, e.g., national research networks such as the Computer Emergency Response Team for the German Research Network DFN (DFN-CERT)
- geographical boundaries, e.g., Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
- organizational boundaries, e.g., SIEMENS-CERT for the organizations in the SIEMENS group
- general public or support for other CSIRT organizations, e.g., CERT/CC and FIRST



Other Issues

Staff

- Incident response staff must have the right combination of skills to be able to work with other team members and within the constituency.

Equipment

- CSIRT staff will need access to basic computing and communications systems to perform their functions.

Infrastructure

- A CSIRT infrastructure should incorporate all known precautions that are physically and financially possible.

© 2001-2004 Carnegie Mellon University

NASCIO Presentation - March 26, 2004 - slide 16

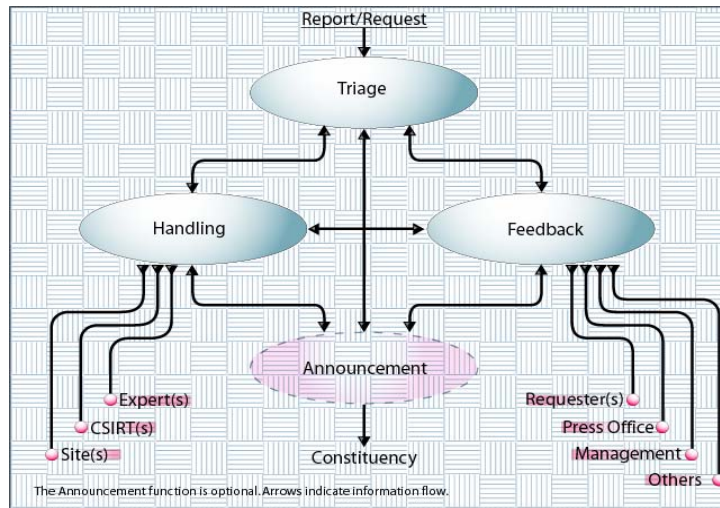
CSIRT resources will include

- skilled staff
 - interpersonal and analysis skills
 - technical skills
 - incident response and security skills

See: *Staffing Your Computer Security Incident Response Team – What Basic Skills Are Needed?* Available at: <http://www.cert.org/csirts/csirt-staffing.html>

- incident reporting and tracking system
- communications mechanisms
 - hotline or helpdesk
 - web site and/or ftp site, mailing distribution lists
 - cell phones and pagers
- secure communications mechanisms
 - PGP keys or digital certificates for signing CSIRT documents and mailings
 - secure remote access, phones, intranets, and extranets
- secured access to CSIRT facilities
- secure infrastructure
 - a firewall to isolate the CSIRT network from the rest of the organization
 - secure network configurations and network security scanners
 - protected power sources, power conditioners and generator (if appropriate)
 - Web, email, and DNS services
- disaster recovery and business resumption plans
- secure off-site back-up location and transportation mechanism

Process Versus Technology



© 2001-2004 Carnegie Mellon University

NASCIO Presentation - March 26, 2004 - slide 17

Incident Handling is not just the application of technology to resolve computer security events.

It is the development of a plan of action, a response plan that

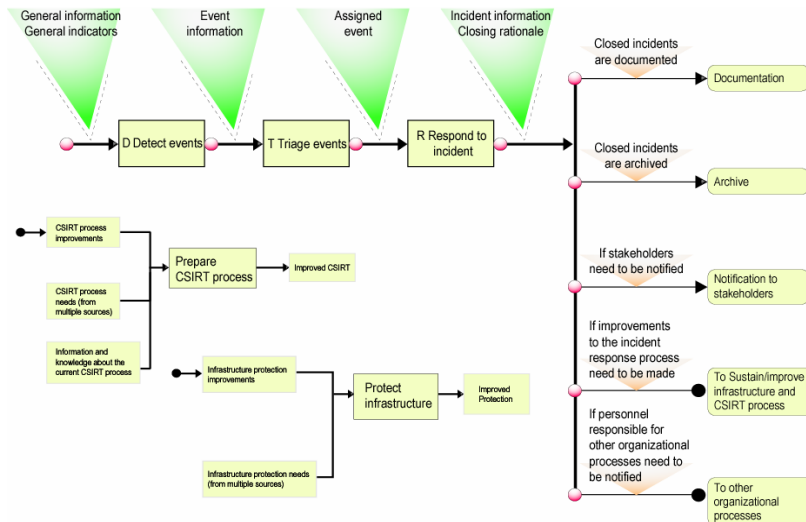
- integrates into the existing processes and organizational structures
- strengthens and improves the capability of the constituency to effectively manage computer security events
- is part of an overall strategy to protect and secure critical business functions and assets

It is the establishment of processes for

- notification and communication
- collaboration and coordination
- analysis and response



Work in Progress: CSIRT Process Mapping



Prepare/Protect

- security awareness training
- incident reporting guidelines
- notification lists
- expertise matrix and non-disclosures
- incident handling tools
- original media and backups
- patch and configuration management systems
- response plans

Detect

- network monitoring and intrusion detection
- constituency reports
- public or private mailing lists

Respond

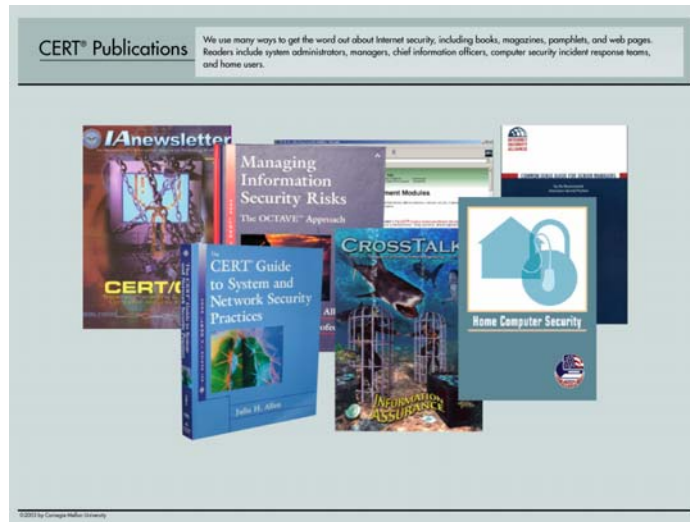
- verify
- contain
- notify
- analyze
- research
- recover
- follow-up

Improve/Sustain

- perform a postmortem
- harden systems
- update response policies and procedures



Resources



© 2001-2004 Carnegie Mellon University

NASCIO Presentation - March 26, 2004 - slide 19

More information can be found in the following publications and at the following sites:

- The Handbook for CSIRTs, Second Edition
<http://www.cert.org/archive/pdf/csirt-handbook.pdf>
- State of the Practice of CSIRTs
<http://www.cert.org/archive/pdf/03tr001.pdf>
- Organizational Models for Computer Security Incident Response Teams (CSIRTs)
<http://www.cert.org/archive/pdf/03hb001.pdf>
- Expectations for Computer Security Incident Response
<http://www.ietf.org/rfc/rfc2350.txt>
- Avoiding the Trial-by-Fire Approach to Security Incidents
<http://www.stsc.hill.af.mil/crosstalk/2000/10/westbrown.html>
- CERT® Coordination Center
<http://www.cert.org/>
- NSS Security Improvement Modules
<http://www.cert.org/security-improvement/>
- Responding to Intrusions
<http://www.cert.org/security-improvement/modules/m06.html>
- US-CERT
<http://www.us-cert.gov/>

Training courses for CSIRT managers and incident handling staff are also available from CERT Training and Education. The schedule and description of courses can be found at <http://www.cert.org/nav/training.html>



Contact Information

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213 USA

Web: <http://www.cert.org/>

Email: cert@cert.org

Hotline: +1 412 268 7090
CERT personnel answer
08:00–17:00
EST(UTC-5)/EDT(UTC-4)
On call for emergencies
during other hours

CERT CSIRT Development Team
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213 USA

Web: <http://www.cert.org/csirts/>

Email: csirt-info@cert.org